VOL 1 (2017) NO 4 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Study on Database Management System Security Issues

Mohd Amin Mohd Yunus [#], Sonniaa K.V. Gopala Krishnan [#], Nazri Mohd Nawi [#], Ely Salwana Mat Surin [*]

[#] Faculty of Science Computer and Information Technology, Universiti Tun Hussein Onn Malaysia, Malaysia
**Institute of Visual Informatic, Universiti Kebangsaaan Malaysia*
E-mail: aminy@uthm.edu.my, elysalwana@ukm.edu.my

***Abstract*—The study is about the security system of database management (DBMS) and proposed method. Information is an essential element in database management system where the users trust service providers will have a secure system to protect and prevent their information from malicious attack or stealing information. There are few types of technique applied to enhance the database security level.**

***Keywords*— Database Management System, security.**

I. INTRODUCTION

Database is an accumulation of data composed in a manner that a computer program can rapidly choose fancied bits of information. User can think about a database as an electronic documenting framework. It’s a set of data which can be access by clients or authorized user in various method. The data are process and stored as information in database management system (DBMS). The information are highly confidential and proprietary of clients. Clients provide the information with trust in the security services of the database that the information will stored safely. A comprehensive strategy to secure a database is more than data security [4]. The usage of security instrument encourages security administrations, recognize and keep a security assault. Security of information stored in database is very crucial in order to avoid unauthorized access. Moreover, the implementation of security service is to identify the unauthorized access, detect any attack on information and part of prevention process. An appropriate method should be apply to secure the data from hack or misuse of data. Data administrator have to provide a well-designed system for clients and person who have the authorization are allow to login to the database management system to add , delete, edit and update the data. There are few types of method can be apply to increase the security level of the information such as limiting the access control where the user have to verify the details with authentication, the period of time used to access the information should be decrease and the data administrator can identify the user to prevent steal of information during the access time. Besides that, maintaining the confidentiality and integrity of the information can apply through watermarking into database. The focus is to detect malicious attacks and for ownerships protection of the information. Watermarking of information can increase the resilient to data manipulation attacks and avoid modification of data without authentication.

II. RELATED WORKS

There are several types of technique for database management system security, the proposed technique is watermarking for ownership. The owner can protect the data by inserting watermark image into database during malicious attack to steal data. In this paper, we investigate a technique for relational database watermarking in which binary image is used as watermark [1]. Besides that, database encryption is the way toward changing over information inside database management system, in plain content configuration into unimportant figure message by methods for an appropriate calculation. The weakly encrypted data are vulnerable to numerous attacks that do not require access to decryption keys [2]. Database decryption is changing over the aimless figure content into the first data utilizing keys produced by the encryption calculations. The purpose of encryption and decryption is to protect the confidentiality of the data and to maintain the data integrity of customers through security services of database. The role of data encrypting is to ensure the confidentiality of data [2]. In addition to, the SecCloud protocol uses encryption for storing data in secure mode [5]. The secrecy of information in cloud services is by limiting the access control and keep track record of information to maintain the security. Although, cloud services does not cost high value but the security, confidentially and integrity of the data is not safe compared to the physical database management system (DBMS). It is difficult to identify the malicious attacks on cloud computing because of its complexity level and dynamic resources which can be access using variety of authentication. This research aims to reduce the risk of unauthorized data access by providing an extra layer of security [3]. It shows the technique of combining the information based on its sensitivity level during designing phase to reduce constraints. The architecture design of a database system must be designed based on the data integrity and security mechanism. An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

III. Proposed Method

Nowadays, the development of digital technology rapidly increases and causes many duplication or change of data like text, image, audio or video. In digital system, duplication of data can generate new data that almost look like the original data. The proposed framework as shown in Figure 1 is to avoid the manipulation and duplication of data for the database security management system (DBMS). The aims of this method is to protect the ownership of the data with implementation of watermarking into database. An image and text will be inserted into the attributes of database in binary form. Then, the invisible watermark image will be embedded with data for copyright purpose. The data will be encrypted and hidden in the system. After that, the encrypted data will be stored and processed. Thus, the user must embed the data with alphabet and numerical characters of secret key. However, the extraction of data will occur after verify the ownership of the pertain data. User must provide accurate information so that the system will decrypt the data for access control. The insertion of watermark will not destroy the original information of the database. Watermarking techniques can be apply by user itself when they provide their data to a system.

The encryption method will perform by creating the watermark algorithm before the embedding process. We will insert a watermark information into the original database and return marked [1]. This method will never change the confidentiality and integrity of the original information. Furthermore, implementing multimedia watermark is easy for large attribute set of data where it can improve the privacy of data.

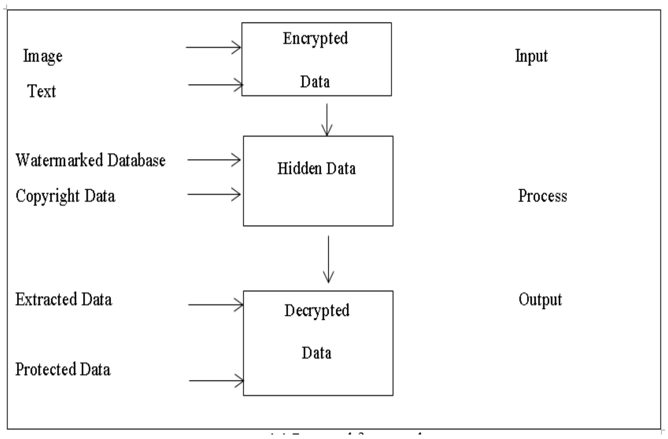
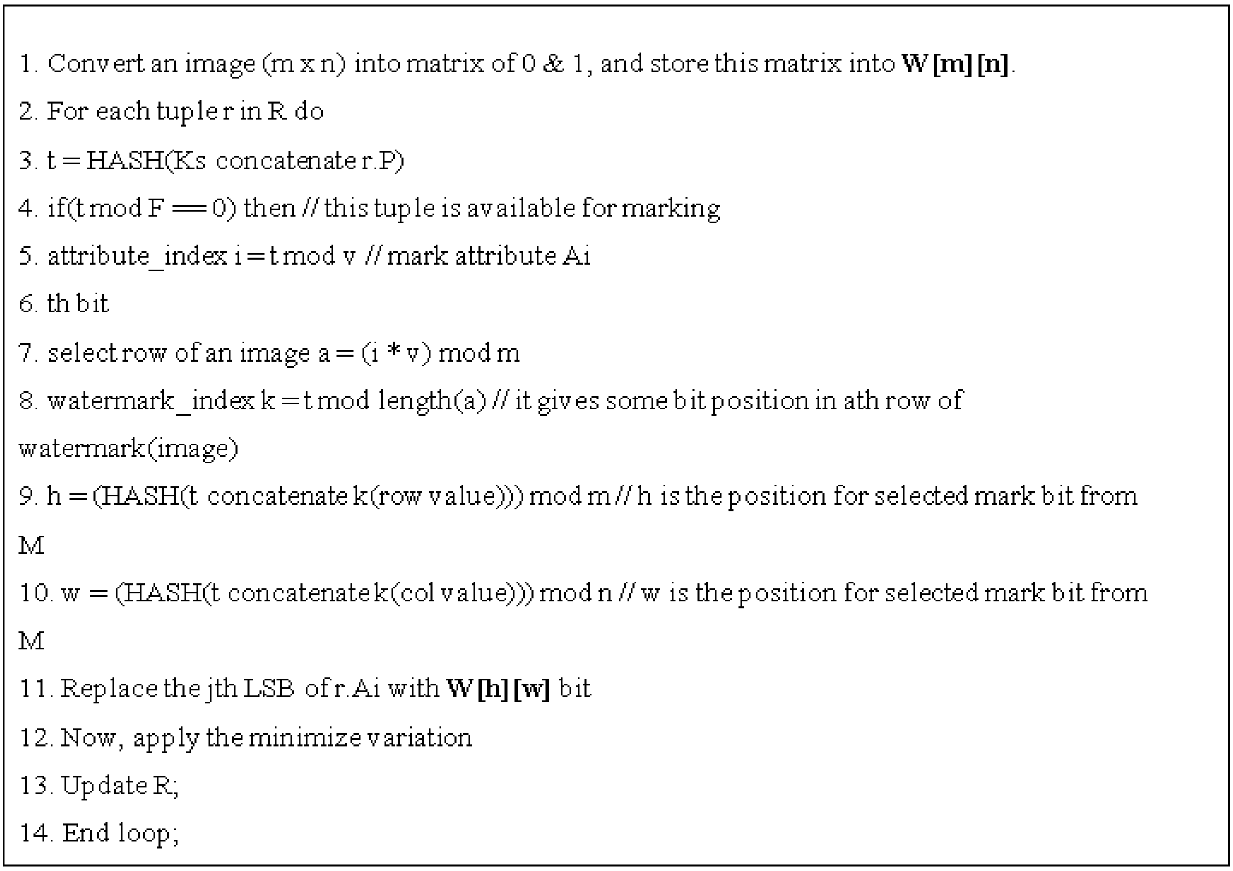


Fig 1. Proposed Data Ownership Protection via DBMS



```
1. Convert an image (m x n) into matrix of 0 & 1, and store this matrix into W[m][n].
2. For each tuple r in R do
3. t = HASH(Ks concatenate r.P)
4. if(t mod F == 0) then // this tuple is available for marking
5. attribute_index i = t mod v // mark attribute Ai
6. th bit
7. select row of an image a = (i * v) mod m
8. watermark_index k = t mod length(a) // it gives some bit position in ath row of
watermark(image)
9. h = (HASH(t concatenate k(row value))) mod m // h is the position for selected mark bit from
M
10. w = (HASH(t concatenate k(col value))) mod n // w is the position for selected mark bit from
M
11. Replace the jth LSB of r.Ai with W[h][w] bit
12. Now, apply the minimize variation
13. Update R;
14. End loop;
```

Fig 2. Watermark Algorithm [1]

IV. DISCUSSION

In this study, the proposed technique can be effective for future works to create a database security mechanism with new approaches. Although, watermarking techniques is widely used to protect multimedia data from manipulation and duplication of audio tracks, videos and photos. Predominantly, multimedia data also stored in database management system. Different types of watermarking provides different level of security. It depends on the crucial point of these data. User can obtain the benefits if the computing system is not expensive where it is designed with proper mechanism. Besides that, image-based watermarking technique was proposed because the image will be insert and convert to be scrambled image in the first phase. Watermarking is mainly focused on ownership due to the data processing level where some of the watermark will be remove or delete by unauthorized party. Moreover, embedded watermark can be used for biometric scan of the content owner only, it can prevent from any distribution without the owner's concern. In this case, the owner is eligible to claim for content copyright's protection if the respective database system has security policy. Watermark also opt for detecting manipulated or any changed data. It is pertinent to ensure the integrity of data is verify through the integrity of extracted data. At the point when database substance is utilized for exceptionally basic applications, for example, business exchanges or therapeutic applications, it is essential to guarantee that the information is provided by correct source without manipulation. This can be accomplished by implanting a watermark in the fundamental information of the database. In general terms, there are two types of watermarking techniques which is watermark embedding and water verification. The first phase is embedding method where the secret key is insert into database and freely accessible without accessing control. Embedding the data using watermark method cannot be applied without exact computing and calculation. The second phase is verifying the authority of the content where the user is required to insert the accurate secret key in order to extract the data from the database. The robustness of the watermarking technique is tested by various malicious attacks.

V. CONCLUSIONS

Precisely, the studies explained on the types of technique that can be used to increase the security level of a database management system (DBMS). The proposed technique is to measure the confidentiality of data is effective or not using this approach. The contributions of the technique are the user can have a secured data without changes and duplication. In addition to, the algorithm method is used by many data administrators in development process. Moreover, watermarking approach can be applied in cloud computing services for high-security mechanism in nearly future. Identifying techniques for ownership protection is an important and challenging task. The proposed technique can be evaluated using database experimental test.

ACKNOWLEDGMENT

This project is indirectly sponsored also by Universiti Tun Hussein Onn Malaysia, This research also supported by Research GATES IT Solution Sdn. Bhd. Under its publication scheme.

REFERENCES

[1] U.P. Rao, D.R. Patel, and P.M. Vikani, “Relational Database Watermarking for Ownership Protection,” Procedia, 6, pp. 988-995 Technology, 2012.

[2] M. Şerban, “Methods to Increase Search Performance for Encrypted Databases,” Procedia Economics and Finance, 3, pp. 1063-1068 (2012)

[3] D. Trivedi, P. Zavarsky, and S. Butakov, “Enhancing Relational Database Security by Metadata Segregation,” Procedia Computer Science, 94, pp. 453-458, 2016.

[4] T.D. Vale, “Principles of Security and Integrity of Databases,” 15, pp. 401-405, 2014.

[5] N. Vurukonda and B.T. Rao, “A Study on Data Storage Security Issues in Cloud,” Computing. Procedia Computer Science, 92, pp. 128-135, 2016.